

**Performance Audit
E-Service Systems Security**

October 2009

**City Auditor's Office
City of Kansas City, Missouri**

October 21, 2009

Honorable Mayor and Members of the City Council:

This performance audit of the city's e-service systems was initiated by the city auditor pursuant to Article II, Section 216 of the city charter. We focused on the controls and security over the city's e-service systems. The city currently offers a number of on-line e-services that businesses and individuals can use to pay earnings taxes, convention and tourism taxes, water bills, as well as traffic and parking tickets. The public is also able to register for Parks and Recreation classes and electronically obtain permits through the city's website. In fiscal year 2009, on-line payments totaled about \$10 million and Automated Clearing House transfers totaled about \$40 million.

The city's e-service systems and data appear to be reasonably secure. An information security assessment performed by an outside firm rated the city's network security above average. The same assessment also identified a number of high risk vulnerabilities in the e-service applications, which were resolved. Another outside firm's assessment determined that the city complies with the payment card industry's data security standards. The periodic external assessments and Information Technology Department's (ITD) corrective actions based on these assessments provide reasonable assurance that the city's e-service systems and related data are secure.

Although ITD follows a number of recommended security practices, ITD's security policies do not always clearly define security responsibilities, some are not included in ITD's written policies and procedures, and the city lacks an entity wide information security management program that encompasses all information security, including application level systems and programs. An overall information security program would provide the foundation for the city's information security control structure and reflect senior management's commitment to addressing security risks. We make several recommendations to improve internal controls related to the city's e-service systems security.

We made a draft of this report available to the city manager and the directors of information technology and finance on September 16, 2009. Management's responses are appended. We would like to thank the Information Technology, Water Services, and Finance departments for their assistance and cooperation during this audit. The audit team for this project was Douglas Jones, Joyce Patton, and Vivien Zhi.

Gary L. White
City Auditor

E-Service Systems Security

Table of Contents

Introduction	1
Objectives	1
Scope and Methodology	1
Background	2
City E-Service Systems	2
Relationship Between Network Security and Application Security	3
Findings and Recommendations	5
Summary	5
E-Service Systems and Data Appear to Be Reasonably Secure	5
Security Assessment Rated City's Network Security Above Average	5
City Complies with Payment Card Industry Data Security Standard (PCI DSS)	7
The City Follows Many Recommended Practices for E-Service Security	7
A Number of Recommended Practices Are in Place	8
More Comprehensive Written Policies Should Be Developed	9
City Lacks an Entity Wide Information Security Management Program	11
Recommendations	13
Appendices	15
Appendix A: Director of Information Technology's Response	15
Appendix B: Director of Finance's Response	19

List of Exhibits

Exhibit 1. On-line Payments – Fiscal Years 2008-2009	3
Exhibit 2. Recommended Practices for E-Service Security	8

Introduction

Objectives

We conducted this audit of the city's e-service systems security under the authority of Article II, Section 216 of the Charter of Kansas City, Missouri, which establishes the Office of the City Auditor and outlines the city auditor's primary duties.

We did this audit because security controls for the city's e-service systems protect the information the systems contain. Businesses and individuals using the on-line systems to make a variety of payments to the city are required to provide credit card numbers, taxpayer identification numbers, social security numbers, business revenue figures, and other personally identifiable information. Unauthorized access to these systems could result in lost/compromised data, service unavailability, or identity theft.

A performance audit provides assurance or conclusions based on an evaluation of sufficient, appropriate evidence against stated criteria. Performance audits provide objective analysis so that management and those charged with governance and oversight can use the information to improve program performance and operations, reduce costs, facilitate decision making, and contribute to public accountability.¹

This report is designed to answer the following question:

- Are the city's e-service systems and related data secured?

Scope and Methodology

Our audit reviewed the control and security of the city's e-service systems, including online wage earner tax filing, municipal court ticket, and water bill pay. Our methods included:

- Interviewing staff in the Information Technology Department (ITD), Finance Department, Water Services Department, and Municipal

¹ Comptroller General of the United States, *Government Auditing Standards* (Washington, DC: U.S. Government Printing Office, 2007), p. 17.

Court to gain an understanding of their concerns, practices, and policies related to securing the city's e-service systems.

- Reviewing the Control Objectives for related Information Technology (COBIT) framework; the Federal Information System Controls Audit Manual (FISCAM); and the Information Systems Audit and Control Association's (ISACA) best practices on e-commerce security to identify criteria and recommended practices for comparison with the city's practices and policies.
- Reviewing the 2008 Kansas City Information Security Assessment Report to identify e-service system vulnerabilities reported to ITD by the consultant.
- Conducting tests of the city's e-service systems to determine whether high risk vulnerabilities identified in the 2008 security assessment were resolved.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

No information was omitted from this report because it was deemed privileged or confidential except for certain information related to the configuration or operation of the e-service systems. State statutes allows this information to be a closed record.²

Background

City E-Service Systems

The city currently offers a number of e-services for making on-line payments.³ Businesses and individual taxpayers can pay their earnings tax through the Kansas City KwikFile and Online Wage Earner systems. The Convention and Tourism Tax System can be used to pay the convention and tourism tax. Residents can pay water bills using the Water Billpay system. Individuals can pay traffic and parking tickets by

² Revised Statutes of Missouri §610.021(20).

³ Other common terms for on-line payments or services are e-commerce or e-government.

using the Municipal Court Ticket System. In addition, the public can register for Parks and Recreation classes and obtain construction-related permits electronically on the city's website. In fiscal year 2009, the city received over \$10 million through on-line credit card payments. (See Exhibit 1.)

Exhibit 1. On-line Payments – Fiscal Years 2008-2009⁴

E-Service Application	2008	2009
Water Billpay	\$7,103,609	\$7,462,604
Municipal Court	1,697,669	2,087,308
Wage Earner	525,957	525,833
City Planning	137,113	123,120
Parks and Recreation	52,883	75,056
Total	\$9,517,231	\$10,273,921

Source: Finance Department records of credit card receipt summaries.

Relationship Between Network Security and Application Security

Network security consists of the provisions made in a computer network infrastructure and policies adopted by the network administrator to protect the network and related services from unauthorized access, modification, destruction, or disclosure and provide for the ongoing monitoring and measurement activities. Network security is generally taken as providing protection at the boundaries of an organization's information or computer system, keeping the intruders out.

Application security is another layer of security that encompasses measures taken to protect an application and related data against unauthorized access or modification of information and includes methods needed to monitor and counter such threats.

⁴ We did not include KwikFile and Convention and Tourism Tax in this table because the city accepts only Automated Clearing House (ACH) transfers for these transactions. On-line KwikFile payments totaled over \$37 million for fiscal year 2009. On-line Convention and Tourism Tax payments totaled over \$3 million for fiscal year 2009.

Findings and Recommendations

Summary

The city's e-service systems and data appear to be reasonably secure. An outside firm performed an information security assessment and rated the city's network security as above average. The same assessment also identified a number of high risk vulnerabilities in the e-service applications, which were resolved by ITD. Another outside firm determined that the city is in compliance with the credit card industry's data security standards. Although ITD follows a number of recommended security practices, the city lacks an entity wide information security management program. Additionally, ITD's security policies do not clearly define security responsibilities. Security for the e-service applications should be a part of an overall information security program, which would provide the foundation for the city's information security control structure and reflect senior management's commitment to addressing security risks.

E-Service Systems and Data Appear to Be Reasonably Secure

A third party assessment rated the city's network security above average. Security for the e-service applications was rated below average but since then, ITD resolved the high and medium risk vulnerabilities. A different external assessment determined that the city complies with the payment card industry's data security standards. The periodic external assessments and ITD's corrective actions based on these assessments provide reasonable assurance⁵ that the city's e-service systems and related data are secure.

Security Assessment Rated City's Network Security Above Average

A security assessment by a third party rated the city's external, internal, and voice networks above average and wireless network average when compared to organizations of similar size. In June 2008, the Information Technology Department (ITD) contracted with an information security firm to conduct an information security assessment for Kansas City.

⁵ Reasonable assurance is the concept that controls, no matter how well designed and operated, cannot provide absolute assurance that controls will always work as designed and that the entity's objectives will be met. Controls should be designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.

This security assessment evaluated the city's external, internal, voice, and wireless networks and application security on the city's e-service systems including Water Billpay, ETax, and Municipal Court Ticket. ITD's information system security policies were also reviewed.

The same security assessment rated security for the e-service applications as below average and identified several application-level security vulnerabilities.⁶ We met with ITD and Water Services staff to discuss the high and medium risk vulnerabilities identified in the security assessment and the corrective action they had taken. ITD hired a contractor to correct the high risk vulnerabilities in the ETax and Municipal Court Ticket systems and Water Services' IT staff corrected the high-risk vulnerabilities in the Water Billpay system. We also conducted limited testing of the e-service systems to verify that corrective actions had been taken to address the high risk security vulnerabilities in the e-service systems. Based on our discussions with responsible staff and limited testing, it appears that the high and medium risk vulnerabilities have been corrected or resolved.

Security assessment results were not shared with staff responsible for maintaining or operating the e-service systems. ITD's security group did not adequately communicate the e-service systems security vulnerabilities identified in the assessment with staff in ITD's web development group or Water Services IT staff who have responsibilities for maintaining the e-service systems. In addition, information from the assessment was not shared with the user departments who own the data.

The ITD security group told the web development group to correct one high-risk vulnerability in the ETax and Municipal Court ticket systems and told Water Services IT to correct a high-risk vulnerability in the Water Billpay system. During a meeting with staff from ITD and Water Services, we learned that the low and moderate risk vulnerabilities were not communicated to the web development group or Water Services IT. ITD also did not inform the Finance Department or Municipal Court (the user departments) about the general nature of the e-service systems vulnerabilities identified in the security assessment or ITD's plan for corrective actions.

⁶ We do not note what these vulnerabilities are as they may identify system configurations or operational parameters that could allow unauthorized access to the e-service systems and related data. This information is a closed record under state statutes (RSMo §610.021(20)).

The results of information security assessments should be communicated to staff who are responsible for maintaining the e-service systems and resolving issues identified in those systems. Without this information, staff responsible for the e-service systems is unaware of potential problems and cannot provide input on how security and other issues can be resolved or corrected. User departments who own the data and systems should be informed about the results in general terms and what corrective actions will be taken. Communicating information about assessment results could lead to a better understanding of issues, quicker resolution of issues, and improved or continued e-services. The director of information technology should develop and implement a policy to improve communication between the ITD security group, ITD web development group, Water Services IT, and user departments about e-service security issues.

City Complies with Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is a worldwide security standard established by the credit card industry. The payment card industry data security standards are technical and operational requirements that were created to help organizations that process credit card payments protect customer account data. ITD has hired a company to perform periodic scans on the city's systems that accept credit card payments to determine whether the city is complying with security standards. The compliance scan is accepted by all the major credit card companies. The city passed the two most recent compliance scans we reviewed.

The City Follows Many Recommended Practices for E-Service Security

Although the city follows a number of recommended e-service security practices, some are not included in ITD's written policies and procedures. We reviewed literature from standards setting bodies and other authoritative sources to develop a set of recommended e-service security practices to compare with city policies and practices. The city follows or partially follows about three-fourths of the recommended practices. (See Exhibit 2.)

Exhibit 2. Recommended Practices for E-Service Security

Recommended Practice	Does the City Follow the Practice?
A regular assessment of the security of e-commerce environments and applications.	Yes
A set of security mechanisms and procedures, such as firewalls, encryption, and password policies.	Yes
Disaster recovery and business continuity plan.	Yes
Physical security for e-commerce servers.	Yes
A policy requiring independent account reconciliation.	Partially. Departments are reconciling the accounts, but there is no written policy.
A policy on segregation of duties.	Partially. There is no formal policy regarding segregation of duties for e-service systems, however, ITD and functional departments segregate incompatible duties.
Access control policies that include periodic reviews.	Partially. ITD's access control policy does not include periodic review of access rights.
A policy on periodic review of audit trails and logs of e-commerce applications.	No. ITD does not do periodic reviews of access logs. However, user departments can request ITD to run access logs.
A comprehensive application security plan.	No

Sources: Control Objectives of related Information Technology (COBIT); ISACA's best practices on e-commerce security; and Federal Information System Control and Audit Manual (FISCAM).

A Number of Recommended Practices Are in Place

ITD has written policies that incorporate several recommended e-service security practices. ITD periodically conducts information security assessments, information system security mechanisms are in place, there is a disaster recovery plan, and physical access to the e-service servers is restricted.

Security assessments are performed periodically. ITD's risk assessment policy states ITD is to perform periodic information security risk assessments for the purpose of determining areas of vulnerability, and to initiate appropriate remediation. ITD has contracted with an information security firm to perform periodic security assessments. The ITD security group routinely performs network vulnerability scans. These assessments and scans provide assurance that controls are present and effective, help identify threats and vulnerabilities, and identify any needed corrective actions to improve system security.

Security mechanisms and procedures are in place. Security mechanisms such as firewalls, encryption, and password management are used to prevent or detect unauthorized access. ITD policies outline the minimum security requirements for hardware and network devices deployed on the city's network. ITD also has a policy on administrative

passwords for desktop PCs and a locking screen saver policy that have been implemented.

Disaster recovery and business continuity plan are in place. ITD has a data backup policy. It includes the backup procedures and how user and departmental data stored on servers and data stored on work stations are handled. In addition, ITD has a data recovery and contingency policy. The policy describes ITD's responsibilities in the event of a problem. Critical ITD applications are included in the citywide emergency plan.

All e-service servers are located at ITD. Physical security restricts physical access to computer resources and protects them from loss or impairment. All the e-service servers are located at ITD. ITD has policies regarding physical access to the building. Visitors to ITD are required to sign in and are accompanied by ITD staff while on the premises.

More Comprehensive Written Policies Should Be Developed

Although a number of recommended practices are being followed by ITD and user departments such as timely reconciliation of on-line payments and segregation of duties, they are not included in ITD's written policies. Access logs for e-service applications are only run when requested by user departments. Access control policies exist but ITD does not review users' access roles and responsibilities periodically.

Departments perform account reconciliations. Although not required by a written policy, the Finance, Municipal Court, and Water Services departments reported that they compare the payments received through their e-service systems to the credit card processor's statement and the settlement account at the bank. Periodic reconciliations ensure that payments received on-line match credits in bank statements and payments are applied to the correct accounts. A written policy on account reconciliations for on-line payments would help ensure that these reconciliations continue. The director of finance should develop and implement written policies and procedures to require departments to reconcile on-line payments to statements from credit card processors and the bank settlement account.

ITD and user departments segregate incompatible duties. Staff in ITD who develop and maintain applications are not responsible for security. Security staff do not develop or maintain applications. In user departments, staff are granted different levels of access rights to prevent them from performing incompatible duties or unauthorized actions.

Although ITD and user departments segregate incompatible duties, ITD does not have a written policy regarding segregation of duties for e-service systems. A written policy would help ensure that incompatible duties continue to be segregated. The director of information technology should develop and implement written policies and procedures to require segregation of duties related to access and use of the city's information assets including the e-service systems.

ITD does not review access logs for e-service systems. An access log or audit trail⁷ has more significance in the e-commerce environment due to the absence of paper trails. Although access logs should be monitored periodically to identify indications of inappropriate or unusual activity in the e-service systems, ITD does not have a policy on monitoring or reviewing them. The director of information technology should develop and implement written policies and procedures to periodically review e-service systems' access logs or audit trails with user departments and investigate inappropriate or unusual activity.

ITD does not review system access rights. Although ITD has an access control policy establishing who is responsible for granting access to city resources such as desktop computers, servers, network devices, firewalls, business applications, and HIPAA data, the city's external auditors recently identified an issue with access control. In the 2008 management letter, the city's external auditors stated that the city did not have an "effective process to periodically review access groups and roles to identify inappropriate or incompatible access rights that conflict with segregation of duties for ITD."⁸ "A periodic review of access is not effectively performed at ITD for key applications."⁸ Management's response to the external audit stated that ITD and the departments would "validate user roles twice yearly for the PeopleSoft applications (both Financials and Human Resources), the Banner system (Water), and ABM (Aviation)."⁹ ITD management reported that they have begun the process for validating user roles for the applications identified by the external auditors, but not the e-service applications.

Access controls provide reasonable assurance that computer resources are protected against unauthorized access, modification, or disclosure; loss; or impairment. Inadequate access controls, such as a lack of effective monitoring efforts, can diminish the reliability of computerized

⁷ An audit trail is a record showing who has accessed a computer system and what operations or actions an individual performed during a given period of time.

⁸ Required Communication and Management Letter from KPMG to the Finance and Audit Committee, April 30, 2008.

⁹ Management Responses to Management Letter Comments from Director of Finance Jeffrey A. Yates to the Mayor, City Council, and City Manager, January 6, 2009.

data and increase the risk of destruction or inappropriate disclosure of data. The director of information technology should coordinate with user departments and periodically perform a review of the access rights for key applications, including the e-services applications, to ensure users' system access and roles are appropriate.

A comprehensive application security plan for the e-service systems has not been defined. Although the city's current security practices over the e-service systems incorporate a number of recommended practices, there is no written policy outlining requirements for e-service systems security. The lack of a comprehensive application security plan for the e-service systems increases the risk of inappropriate access, compromised confidentiality, and reduced system availability.

A written application security plan would provide a framework for e-service system security management that identifies and describes applications, assigns roles and responsibilities, documents security policies and procedures, assesses security risks, performs ongoing monitoring activities, and coordinates with entity wide security policies for security. The director of information technology should develop and implement an application security plan for the e-service systems and related data.

City Lacks an Entity Wide Information Security Management Program

During work that focused on e-service security and ITD's policies and procedures for those systems, we also found that there is no entity wide information security management program in place that encompasses all information security, including application level systems and programs. An overall security program would establish a framework and ongoing cycle of risk assessment, security procedure development and implementation, and monitoring activities. Although ITD has a number of policies, procedures, and practices, these mainly focus on the technical aspects of the operation rather than a comprehensive security program.

An entity wide information security management program provides the foundation for the information security control structure and reflects senior management's commitment to addressing security risks to the city's information assets. The security management program should cover all major systems and facilities and outline the duties and responsibilities for who oversees information security as well as those who own, use, or rely on the city's information resources. For example, ITD is responsible for information technology, but individual

departments are often the owners of the applications and data that are generated using the technology.

Establishing an entity wide information security management program will provide the city manager with an opportunity to demonstrate that safeguarding city information assets is a priority. It is important that the city manager establish the program because responsibility and authority need to be defined for both ITD and user departments. The city's information security consultant recommended in the 2008 assessment, that a statement regarding management's commitment to information security was needed and roles and responsibilities should be further defined.

Without an information security management program, security controls could be inadequate; roles and responsibilities unclear, misunderstood, or improperly implemented; and controls inconsistently applied or monitored. Such conditions can increase the risk that systems and data will not be adequately protected. The city manager should develop and implement an entity wide information security management program. The program should clearly define responsibilities for data security, define accountability for developing and implementing information security policies and practices, establish a framework and continuing cycle of activity for assessing risk, and outline processes to monitor the effectiveness of information security procedures.

Recommendations

1. The city manager should develop and implement an entity wide information security management program.
2. The director of information technology should develop and implement written policies and procedures that outline segregation of duties requirements for city information assets.
3. The director of information technology should periodically review access logs or audit trails and users' access rights to key applications, including the e-service systems, with user departments.
4. The director of information technology should establish an application security plan for the e-service systems and related data.
5. The director of information technology should ensure that the ITD security group communicates e-service security issues to the ITD web development group, Water Services IT, and user departments.
6. The director of finance should develop and implement written policies and procedures to require departments to reconcile on-line payments to statements from credit card processors and the bank settlement account.

Appendix A

Director of Information Technology's Response



Information Technology Department

DATE: October 6th, 2009
TO: Gary White, City Auditor
FROM: Ivan Drinks Sr., CIO 
SUBJECT: E-Services Audit - 2009



My staff and I have reviewed the recommendations and offer the following responses.

1. The City Manager should develop and implement an entity wide information security management program.
 - a. Agrees. While ITD can contribute information on policies for securing the City's technology assets, this information needs to be combined, reviewed and updated to create a single AR for an entity wide policy. ITD estimates it can deliver a proposed entity wide information security management program to the City Manager for review by March 1, 2010.
2. The director of information technology should develop and implement written policies and procedures that outline segregation of duties requirements for city information assets.
 - a. ITD agrees. ITD currently has policies and procedures for individual applications that reference the separation of these duties. ITD will create a compensative policy and procedure for implement by February 1st, 2010.
3. The director of information technology should periodically review access logs or audit trails and users access rights to key applications, including the e-service systems, with user departments.
 - a. ITD agrees. ITD will expand its policy and procedure in place for the financial system to all applications. This will be implemented immediately.
4. The director of information technology should establish an application security plan for the e-service systems and related data.
 - a. ITD agrees. As stated in #1, ITD will develop a proposed security management program that includes all levels of technology assets.

5. The director of information technology should ensure that the ITD security group communications e-services security issues to the ITD web development group, Water services IT, and user departments.
 - a. ITD agrees. ITD Executive Management will work with the groups listed to identify the current breakdown in communication and create a communication plan for all areas of service related to e-services. ITD anticipates a completion date by January 1, 2010.

Appendix B

Director of Finance's Response

CITY OF FOUNTAINS
HEART OF THE NATION



KANSAS CITY
MISSOURI

Finance Department



DATE: October 7, 2009
TO: Gary White, City Auditor
FROM: Jeffrey A. Yates, CFO/Director of Finance
RE: E-Commerce Audit Finding #6

The Director of Finance should develop and implement written policies and procedures to require departments to reconcile on-line payments to statements from credit card processors and the bank settlement account.

Management agrees with this comment, the Director of Finance will prepare a Management Instruction (MI) directing regular reconciliations of these and other accounts.

c: Wayne A. Cauthen, City Manager
Charles Eddy, Chief of Staff
Randall J. Landes, City Treasurer
Wanda J. Gunter, Acting Commissioner of Revenue/Deputy Director of Finance
G. Mary Temple, City Controller